A Substructural Epistemic Resource Logic

Didier Galmiche*, Pierre Kimmel*, and David Pym†

*Université de Lorraine, LORIA, France †University College London, UK

Abstract We present a substructural epistemic logic, based on Boolean BI, in which the epistemic modalities are parametrized on agents' local resources. The new modalities can be seen as generalizations of the usual epistemic modalities. The logic combines Boolean BI's resource semantics with epistemic agency. We give a labelled tableaux calculus and establish soundness and completeness with respect to the resource semantics. We illustrate the use of the logic by discussing an example of side-channels in access control using resource tokens.

1 Introduction

The concept of resource is important in many fields including, among others, computer science, economics, and security. For example, in operating systems, processes access system resources such as memory, files, processor time, and bandwidth, with correct resource usage being essential for the robust function of the system. The internet can be regarded as a giant, dynamic net of resources, in which Uniform Resource Locators refer to located data and code. In recent years, the concept of resource has been studied and analysed in computer science through the bunched logic, BI, [14] and its variants, such as Boolean BI (BBI) [15] and applications, such as Separation Logic [15,21]. The *resource semantics* — i.e., the interpretation of BI's semantics in terms of resources — that underpins these logics is mainly concerned sharing and separation, corresponding to additive, such as $\wedge$, and multiplicative connectives, such as $*$, respectively. These logics are the logical kernels of the separating, or separation, logics, with resources being interpreted in various ways, such as memory regions, [15,21] or elements of other particular monoids of resources [3].

The logic BI of bunched implications — see, for example, [11,14,20] — freely combines intuitionistic propositional additives with intuitionistic propositional multiplicatives. In Boolean BI (BBI) [15], the additives are classical. The key feature of BI as a modelling tool, and hence of its specific model Separation Logic, is its control of the representation and handling of resources provided by the resource semantics and the associated proof systems. BI's basic propositional connectives come in two groups. The additives, which can be handled either classically or intuitionistically, are familiar disjunction, conjunction, and implication. For example,

$$r \models \phi \wedge \psi \text{ iff } r \models \phi \text{ and } r \models \psi.$$

The key point here is that the resource r is *shared* between the two components of the disjunction.

In contrast, the multiplicative conjunction, $*$, divides the resource between its propositional components, using a partial commutative monoidal operation, $\circ$,

$$r \models \phi * \psi \text{ iff there are } s \text{ and } t \text{ such that } r = s \circ t \text{ and } s \models \phi \text{ and } t \models \psi.$$

That is, the monoid specifies a *separation* of the resources between the components of the conjunction. In Separation Logic, where the semantics is built out of sets of memory locations, the two resource components are required to be disjoint. Details may be found in the references given above.

BI's sequent proof systems employ *bunches*, with two context-building operations: one for the additives (characterized by $\wedge$, which admits weakening and contraction) and one for the multiplicatives (characterized by $*$, which admits neither weakening nor contraction), leading to the following rules for the corresponding implications, $\rightarrow$ and $-\!\!*$:

$$\frac{\Gamma; \phi \vdash \psi}{\Gamma \vdash \phi \rightarrow \psi} \qquad \text{and} \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi -\!\!* \psi}.$$

Again, details may be found in the references given above.

The soundness and completeness of BI for the semantics given above is established in [20] and via labelled tableaux in [11], and the completeness of BBI for the partial monoid semantics described above is established in [16].

Modal extensions of BI, such as MBI [1,3], DBI, and DMBI [6], have been proposed to introduce dynamics into resource semantics. In recent work, the idea of introducing agents, together with their knowledge, into the resource semantics has led to an Epistemic Separation Logic, called ESL, in which epistemic possible worlds are considered as resources [7]. This logic corresponds to an extension of Boolean BI with a knowledge modality, K_a, such that $K_a\phi$ means that the agent a knows that ϕ holds.

Various previous works on epistemic logics consider the concept of resource, using a variety of approaches. They include [2,13,17]. Here we aim to explore more deeply the idea of epistemic [9] reasoning in the context of resource semantics, and its associated logic, by taking the basic epistemic modality K_a and parametrizing it with a resource s, with the associated introduction of relations not only between resources, according to an agent, but also between composition of resources in different ways. The parametrizing resource may be thought of as being associated with, or local to, the agent. This approach leads to the definition of three new modalities $\mathbf{L}^s_a$, $\mathbf{M}^s_a$, and $\mathbf{N}^s_a$ and, consequently, to a new logic in which, as a leading example, we can obtain an account of access to resources and its control, whether they be pieces of knowledge, locations, or other entities. We call this logic *Epistemic Resource Logic* or ERL.

In Section 2, we set up the logic ERL by a semantic definition and, in Section 3, we give the key conservative extension properties of the logic. In Section 4, we explain, how to use the logic to model and reason about the relationship between a security policy — in the context of access control — and the system to which it is applied (cf. [22]). Our application to systems security policy stands in contrast to other work (e.g., [19]) in which epistemic logic has been applied to the analysis of cryptographic protocols. In Section 5, we set up a labelled tableaux calculus for ERL, and establish soundness with respect to ERL's semantic definition and also completeness from a countermodel extraction method. Details of the arguments are provided in [12].

2 An Epistemic Resource Logic

The language $\mathcal{L}$ of the epistemic resource logic, or ERL, is obtained by adding two new modal operators $\mathbf{L}$ and $\mathbf{M}$ to the BI language. In order to define the language of ERL, we introduce the following structures: a finite set of agents A; a finite set of resources *Res*, with a particular element, e; an internal composition operator $\cdot$ on *Res* ($\cdot : Res \times Res \rightharpoonup Res$); a countable set of propositional symbols Prop. The language $\mathcal{L}$ of ERL is defined as follows:

$$\phi ::= \mathrm{p} \mid \bot \mid \top \mid \neg\phi \mid \mathrm{I} \mid \phi \vee \psi \mid \phi \wedge \psi \mid \phi \rightarrow \phi \mid \phi * \phi \mid \phi \mathrel{-\!\!*} \phi \mid \mathbf{L}^s_a\phi \mid \mathbf{M}^s_a\phi$$

where $\mathrm{p} \in \mathrm{Prop}$, $a \in A$ and $s \in Res$. We also define the following operators: $\mathbf{N}^s_a\phi \equiv \mathbf{L}^s_a(\mathbf{M}^s_a\phi)$, $\widetilde{\mathbf{M}}^s_a\phi \equiv \neg\mathbf{M}^s_a\neg\phi$, $\widetilde{\mathbf{L}}^s_a\phi \equiv \neg\mathbf{L}^s_a\neg\phi$, $\widetilde{\mathbf{N}}^s_a\phi \equiv \neg\mathbf{N}^s_a\neg\phi$. The meanings of these connectives are defined in the sequence of definitions that follow below. For simplicity, we write rs instead of $r \cdot s$ and so write $\mathbf{L}^{rs}_a\phi$ instead of $\mathbf{L}^{r\cdot s}_a\phi$.

Note that we introduce modalities that depend on agents and resources, and compare them with previous work on an epistemic extension of Boolean BI [7]. With a slight abuse of notation, we have explicit resources in the language syntax: just as in [8], we must assume that the resource elements present in the syntax of the modalities have counterparts in the partial resource monoid semantics. This design choice has consequences both for the expressivity of the logic and for the formulation of the tableaux calculus.

Definition 1 (Partial resource monoid). *A* partial resource monoid *(PRM) is a structure $\mathcal{R} = (R, \bullet)$ such that*

- *R is a set of* resources *such that $Res \subseteq R$ (which notably means that $e \in R$), and*
- *$\bullet : R \times R \rightharpoonup R$ is an operator on R such that, for all $r_1, r_2, r_3 \in R$,*
  - *$\bullet$ is an extension of $\cdot$: if $r_1, r_2, r_3 \in Res$, then $r_1 = r_2 \cdot r_3$ iff $r_1 = r_2 \bullet r_3$,*
  - *e is a neutral element: $r_1 \bullet e \downarrow$ and $r_1 \bullet e = r_1$,*
  - *$\bullet$ is commutative: if $r_1 \bullet r_2 \downarrow$, then $r_2 \bullet r_1 \downarrow$ and $r_2 \bullet r_1 = r_1 \bullet r_2$, and*
  - *$\bullet$ is associative: if $r_1 \bullet (r_2 \bullet r_3) \downarrow$, then $(r_1 \bullet r_2) \bullet r_3 \downarrow$ and $(r_1 \bullet r_2 \bullet) r_3 = r_1 \bullet (r_2 \bullet r_3)$.*

Here $r \bullet r' \downarrow$ means $r \bullet r'$ is defined. We call e the *unit resource* and $\bullet$ the *resource composition*. Henceforth, $\wp(S)$ denotes the powerset of S.

Definition 2 (Model). *A* model *is a triple $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a\in A}, V)$ such that*

- *$\mathcal{R} = (R, \bullet)$ is a PRM,*
- *for all $a \in A$, $\sim_a \subseteq R \times R$ is an equivalence relation, and*
- *$V : \mathrm{Prop} \to \wp(R)$ is a valuation function.*

We can place this logic in the context of our previous work on modal [3,4] and epistemic extensions of (Boolean) BI [6,7]. In [7], an epistemic extension of Boolean BI, called ESL, is introduced. In this logic, there is just one epistemic modality, K_a, which allows the knowledge of an agent a to be expressed. More formally, the semantics of this modality is defined by $r \models_{\mathcal{W}} K_a\phi$ if and only if, for all r' such that $r \sim_a r'$, $r' \models_{\mathcal{W}} \phi$, where r and r' are semantic worlds (or resources) and $\sim_a$ is a relation between

worlds that expresses that they are equivalent from the point of view of the agent a. This parametrization of modality on resource derives from ideas that are conveniently expressed in, for example, [3,4].

In this paper, we aim to develop the idea in order to consider a modality like K_a and to parametrize it on a resource s, requiring the world relation to be of the form $r \bullet s \sim_a r'$ or $r \sim_a r' \bullet s$ or even $r \bullet s \sim_a r' \bullet s$. Then, in the spirit of ESL, we define a new logic from Boolean BI that allows us to model not only relations between resources according to an agent, but also how those relations are restricted by resources. We can also consider the resources upon which the agent's relation are parametrized to be local to the agent.

In this spirit, we define three new modalities $\mathbf{L}^s_a\phi$, $\mathbf{M}^s_a\phi$, and $\mathbf{N}^s_a\phi$, for which we have the following semantics expressing the evident three forms of the agent's contingency for truth in the presence of composable resources:

1. $\mathbf{L}^s_a\phi$ expresses that the agent, a, can establish the truth of ϕ using a given resource whenever the ambient resource, r, can be combined with the agent's local resource, s, to yield a resource that a judges to be equivalent to that given resource:

$$r \models_{\mathcal{W}} \mathbf{L}^s_a\phi \text{ iff for all } r' \text{ such that } r' \sim_a r \bullet s,\ r' \models_{\mathcal{W}} \phi.$$

2. $\mathbf{M}^s_a\phi$ expresses that the agent, a, can establish the truth of ϕ using a resource that is the combination of its local resource, s, with any resource such that a judges the combined resource to be equivalent to the ambient resource, r:

$$r \models_{\mathcal{W}} \mathbf{M}^s_a\phi \text{ iff for all } r' \text{ such that } r' \bullet s \sim_a r,\ r' \bullet s \models_{\mathcal{W}} \phi.$$

3. $\mathbf{N}^s_a\phi$ expresses that the agent, a, can establish the truth of ϕ using any resource combined with its local resource, s, provided a judges that combination to be equivalent to the combination of that resource with the ambient resource, r:

$$r \models_{\mathcal{W}} \mathbf{N}^s_a\phi \text{ iff for all } r' \text{ such that } r' \bullet s \sim_a r \bullet s,\ r' \bullet s \models_{\mathcal{W}} \phi.$$

ERL can thus be seen as a particular epistemic logic that provides new modalities which model access to resources, whether they are interpreted as pieces of knowledge, locations, or otherwise.

Definition 3 (Satisfaction and validity). *Let $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a\in A}, V)$ be a model. The satisfaction relation $\models_{\mathcal{W}} \subseteq R \times \mathcal{L}$ is defined, for all $r \in R$, as follows:*

$$\begin{array}{ll} r \models_{\mathcal{W}} \mathrm{p} \quad \text{iff} \quad r \in V(\mathrm{p}) & r \models_{\mathcal{W}} \phi \vee \psi \text{ iff } r \models_{\mathcal{W}} \phi \text{ or } r \models_{\mathcal{W}} \psi \\ r \models_{\mathcal{W}} \bot \text{ never} & r \models_{\mathcal{W}} \phi \wedge \psi \text{ iff } r \models_{\mathcal{W}} \phi \text{ and } r \models_{\mathcal{W}} \psi \\ r \models_{\mathcal{W}} \top \text{ always} & r \models_{\mathcal{W}} \phi \to \psi \text{ iff if } r \models_{\mathcal{W}} \phi, \text{ then } r \models_{\mathcal{W}} \psi \\ r \models_{\mathcal{W}} \neg\phi \quad \text{iff} \quad r \not\models_{\mathcal{W}} \phi & \end{array}$$

$$r \models_{\mathcal{W}} \mathrm{I} \text{ iff } r = e$$
$$r \models_{\mathcal{W}} \phi * \psi \text{ iff there exist } r_1, r_2 \in R \text{ s.t. } r_1 \bullet r_2 \downarrow,\ r_1 \bullet r_2 = r, \text{ and } r_1 \models_{\mathcal{W}} \phi \text{ and } r_2 \models_{\mathcal{W}} \psi$$
$$r \models_{\mathcal{W}} \phi \mathrel{-\!\!*} \psi \text{ iff for all } r' \in R, \text{ if } r \bullet r' \downarrow \text{ and } r' \models_{\mathcal{W}} \phi, \text{ then } r \bullet r' \models_{\mathcal{W}} \psi$$

$$r \models_{\mathcal{W}} \mathbf{L}^s_a\phi \text{ iff for all } r' \in R, \text{ if } r \bullet s \sim_a r', \text{ then } r' \models_{\mathcal{W}} \phi$$
$$r \models_{\mathcal{W}} \mathbf{M}^s_a\phi \text{ iff for all } r' \in R, \text{ if } r \sim_a r' \bullet s, \text{ then } r' \bullet s \models_{\mathcal{W}} \phi$$
$$r \models_{\mathcal{W}} \mathbf{N}^s_a\phi \text{ iff } \textit{for all } r' \textit{ such that } r' \bullet s \sim_a r \bullet s,\ r' \bullet s \models_{\mathcal{W}} \phi.$$

A formula ϕ *is* valid*, denoted* $\vDash \phi$*, if and only if, for all* $\mathcal{M}$ *and all* r, $r \models_{\mathcal{W}} \phi$.

Note that $\mathbf{N}^s_a\phi \equiv \mathbf{L}^s_a(\mathbf{M}^s_a\phi)$. To see this, consider that $r \models_{\mathcal{W}} \mathbf{L}^s_a(\mathbf{M}^s_a\phi)$ iff, for all $r' \in R$, if $r \bullet s \sim_a r'$, then $r' \models_{\mathcal{W}} \mathbf{M}^s_a\phi$ iff, for all $r' \in R$, if $r \bullet s \sim_a r'$, then, for all $r'' \in R$, if $r' \sim_a r'' \bullet s$, then $r'' \bullet s \models_{\mathcal{W}} \phi$ iff, for all $r', r'' \in R$, if $r \bullet s \sim_a r'$ and $r' \sim_a r'' \bullet s$, then $r'' \bullet s \models_{\mathcal{W}} \phi$ iff (by the transitivity of $\sim_a$), for all $r'' \in R$, if $r \bullet s \sim_a r'' \bullet s$, then $r'' \bullet s \models_{\mathcal{W}} \phi$ iff $r \models_{\mathcal{W}} \mathbf{N}^s_a\phi$.

Proposition 1 (Satisfaction for the secondary modalities). *Let* $\mathcal{M} = (\mathcal{R}, \{\sim_a\}_{a\in A}, V)$ *be a model, and let* $r \in R$*. The following statements hold:*

1. $r \models_{\mathcal{W}} \widetilde{\mathbf{L}}^s_a\phi$ *iff there exists* $r' \in R$ *such that* $r \bullet s \sim_a r'$ *and* $r' \models_{\mathcal{W}} \phi$*;*
2. $r \models_{\mathcal{W}} \widetilde{\mathbf{M}}^s_a\phi$ *iff there exists* $r' \in R$ *such that* $r \sim_a r' \bullet s$ *and* $r' \bullet s \models_{\mathcal{W}} \phi$*;*
3. $r \models_{\mathcal{W}} \widetilde{\mathbf{N}}^s_a\phi$ *iff there exists* $r' \in R$ *such that* $r \bullet s \sim_a r' \bullet s$ *and* $r' \bullet s \models_{\mathcal{W}} \phi$.

Proof. For example, consider the first part. $\widetilde{\mathbf{L}}^s_a\phi \equiv \neg\mathbf{L}^s_a\neg\phi$, so $r \models_{\mathcal{W}} \widetilde{\mathbf{L}}^s_a\phi$ iff $r \models_{\mathcal{W}} \neg\mathbf{L}^s_a\neg\phi$ iff $r \not\models_{\mathcal{W}} \mathbf{L}^s_a\neg\phi$ iff there exists $r' \in R$ s.t. $r \bullet s \sim_a r'$ and $r' \not\models_{\mathcal{W}} \neg\phi$ iff there exists $r' \in R$ s.t. $r \bullet s \sim_a r'$ and $r' \models_{\mathcal{W}} \phi$. Parts 2 and 3 are similar.

Note that the first point of the definition of $\bullet$, in Definition 1, implies that the three other definitions (neutral element, commutativity, and associativity) extend to $\cdot$, so that the following are semantically equivalent (i.e., every valid formula in the one is valid in the other) for any agent a and any resources r, s, and t: $\mathbf{L}^{re}_a\phi \equiv \mathbf{L}^r_a\phi$, $\mathbf{L}^{rs}_a \equiv \mathbf{L}^{sr}_a$, and $\mathbf{L}^{r(st)}_a \equiv \mathbf{L}^{(rs)t}_a$. Of course, these equivalences also hold for $\mathbf{M}\phi$, $\mathbf{N}\phi$, $\widetilde{\mathbf{L}}\phi$, $\widetilde{\mathbf{M}}\phi$, and $\widetilde{\mathbf{N}}\phi$.

3 Some Properties of ERL

Consider two fragments of ERL. First, $\mathrm{ERL}_{\mathrm{BBI}}$ — corresponding to BBI [15] — with $A = \emptyset$ on the language $\mathcal{L}_{|BBI}$ defined as $\mathcal{L}$ excluding the $\mathbf{L}$, $\mathbf{M}$, and $\mathbf{N}$ operators. Second, $\mathrm{ERL}_{\mathrm{EL}}$ — corresponding to the epistemic logic EL consisting of classical propositional additives and the basic epistemic operator $\mathbf{K}_a$ [9] — with $Res = \{e\}$, on the language $\mathcal{L}_{|EL}$ defined as $\mathcal{L}$ excluding I, $*$, and $-\!\!*$ and with $\mathbf{L}$, $\mathbf{M}$, and $\mathbf{N}$ replaced by the operator $\mathbf{K}_a$, which is defined, for all agents a, by $\mathbf{K}_a\phi = \mathbf{L}^e_a\phi = \mathbf{M}^e_a\phi$.

Proposition 2 (ERL is a conservative extension of BBI and EL). *If, in every model of BBI, the neutral element of the composition is the element e of Res, then* $\mathrm{ERL}_{\mathrm{BBI}}$ *is semantically equivalent to Boolean BI (BBI). If the agent sets are the same for the two languages,* $\mathrm{ERL}_{\mathrm{EL}}$ *is semantically equivalent to the epistemic logic EL.*

Definition 4. *The logic* ERL^* *is defined as ERL but with the addition of the two following properties to the partial resource monoid (Definition 1): 1.* $\bullet$ *has the right-composition property, namely, if* $r_1 = r_2$ *and* $r_1 \bullet r_3 \downarrow$*, then* $r_2 \bullet r_3 \downarrow$ *and* $r_2 \bullet r_3 = r_1 \bullet r_3$*; 2.* $\bullet$ *has the right-cancellation property, namely, if* $r_1 \bullet r_3 = r_2 \bullet r_3$*, then* $r_1 = r_2$.

Note that left-cancellation and left-composition also hold trivially, as $\bullet$ is commutative.

Lemma 1. *Let $a \in A$ be an agent, $r,s \in Res$ be resources and ϕ be a formula of* ERL*. *We have the following equalities:*

1. $\mathbf{L}^t_a(\mathbf{L}^s_a\phi) \equiv \mathbf{L}^{ts}_a\phi$
2. $\mathbf{M}^t_a(\mathbf{M}^s_a\phi) \equiv \mathbf{M}^s_a\phi$
3. $\mathbf{M}^t_a(\mathbf{L}^s_a\phi) \equiv \mathbf{L}^s_a\phi$
4. $\mathbf{N}^t_a(\mathbf{N}^s_a\phi) \equiv \mathbf{L}^t_a(\mathbf{N}^s_a\phi)$
5. $\mathbf{L}^e_a\phi \equiv \mathbf{M}^e_a\phi \equiv \mathbf{N}^e_a\phi$
6. $\widetilde{\mathbf{L}}^t_a(\widetilde{\mathbf{L}}^s_a\phi) \equiv \widetilde{\mathbf{L}}^{ts}_a\phi$
7. $\widetilde{\mathbf{M}}^t_a(\widetilde{\mathbf{M}}^s_a\phi) \equiv \widetilde{\mathbf{M}}^s_a\phi$
8. $\widetilde{\mathbf{M}}^t_a(\widetilde{\mathbf{L}}^s_a\phi) \equiv \widetilde{\mathbf{L}}^s_a\phi$
9. $\widetilde{\mathbf{N}}^t_a(\widetilde{\mathbf{N}}^s_a\phi) \equiv \widetilde{\mathbf{L}}^t_a(\widetilde{\mathbf{N}}^s_a\phi)$.

Proof. Straightforward calculations using the semantic definitions of the modalities.

4 Modelling with the Logic ERL

Using a very simple, well-known example, we illustrate how to use ERL, and its special fragment ERL*, in modelling access control situations. There is often a gap between theory and practice when dealing with security matters. Specifically, when a particular security *policy* is applied to a particular *system*, the behaviour of the system may not be as intended.

Consider the example of Schneier's gate, [22], wherein a security system is ineffective because of the existence of a side-channel that allows a control to be circumvented. Here a facility that is intended to be secured is protected by a barrier that prevents cars from entering into the facility. The barrier may be controlled by a token — such as a card, a remote, or a code — the holding of which distinguishes authorized personnel from intruders. If, however, the barrier itself is surrounded by ground that can be traversed by a vehicle, without any kind of fence or wall, then any car can drive around it (whether it's with a malicious intent or just by laziness of getting through the security procedure) and the access control policy, as implemented by the barrier and the tokens, is undermined. So, the access control policy — that only authorized personnel, in possession of a token, may take vehicles into the facility — is undermined by the architecture of the system to which it is applied.

We show how ERL* can be used to model, and so reason about, the situation described above (following [22]), illustrating how such situations can be identified by logical analysis. Related analyses, employing logical models of layered graphs, can be found in [5]. We start with a simple model, depicted in Figure 1, and gradually refine it. We model just a facility protected by an access barrier. A vehicle having the appropriate access token should be able to get inside. Here we use resources to represent various entities in the model and the atomic formulae characterize properties on those entities. A substantive explanation of systems modelling using locations, resources, processes, and associated substructural modal logics may be found in [1,3]. We consider the following sets of resources, agents, and properties: $Res = \{e,t,b\}$, $A = \{a\}$, $\text{Prop} = \{O,J\}$. O and J respectively express being *outside* and *inside* the facility (we use J instead of I to avoid confusion with I, the unit operator). If a resource $c \in R$ represents a vehicle, $c \models_{\mathcal{W}} O$ means that c is outside the facility, and $c \models_{\mathcal{W}} J$ means it is inside. The agent a is a generic one that represents a user of the system. The resources b and t represent tokens that stand respectively for the barrier and the access token of the users.

From the modelling perspective, the resources we have exposed here are diverse in nature: t is a material token (key or card for instance), c represents a car, while b seems

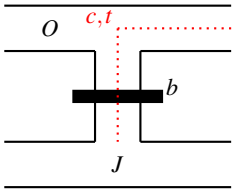

Figure 1. Barrier problem, base case

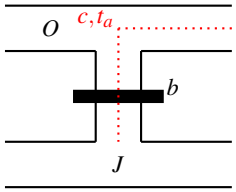

Figure 2. Barrier problem with agents

to be just a marker for the presence or well-functioning of the barrier. This diversity raises the question of the meaning and value of the neutral resource e. We elide that problem by accepting that resources encompass a variety of different objects, but we can also employ the epistemic nature of our logic and consider that resources represent not objects as such but rather the knowledge that a given object is in our system. For example, c can be viewed as an abstract token marking the presence of a car, and t the presence of the required access device in this car. Thus resources act as an abstraction layer of our system. In that view, it's easy to see e as the absence of information (we know nothing of our system).

We have the following property: $O \to \mathbf{L}_a^{bt} J$. According to the semantics, based on a resource monoid R, $c \models_{\mathcal{W}} O \to \mathbf{L}_a^{bt} J$ just in case if $c \models_{\mathcal{W}} O$, then, for every $c' \in R$ such that $c \bullet b \bullet t \sim_a c'$, $c' \models_{\mathcal{W}} J$. Thus the combination of the two tokens grants access to the inside. The use of the token b for the presence of the barrier helps in modelling a situation in which the barrier is completely shut or is broken (in which case entering wouldn't be possible). Note that the formulae $O \to \mathbf{L}_a^{t} J$, $O \to \mathbf{L}_a^{b} J$, and $O \to \mathbf{L}_a^{e} J$ are not valid because we cannot enter if the barrier is shut, if we have no access token, or both.

The use of the operator $\mathbf{L}$ in this situation is illustrative. First, consider what differences the use of one of the other two operators would make. If we were to state $O \to \mathbf{M}_a^{bt} J$, then it would mean that anyone outside can get (without condition) inside and acquire the two access tokens. This is of course not what we expect. On the other hand, using $\mathbf{N}$ has an interesting effect. $O \to \mathbf{N}_a^{bt} J$ requires not only that an entering agent have the expected tokens, but also that those tokens remain active once they are inside. This is slightly different from our first approach: we don't know if the tokens are still active once the agent is inside.

We can also consider which of the additive implication, $\to$, and the multiplicative, $-\!\!*$, would be the better modelling choice in this example. For a first approach, $\to$ seems quite sufficient. Indeed, if we assert $O \to \mathbf{L}_a^{bt} J$ as valid, then any resource satisfies it. So, if we have a car c such that $c \models_{\mathcal{W}} O$, we also have $c \models_{\mathcal{W}} O \to \mathbf{L}_a^{bt} J$, and then we get the expected $c \models_{\mathcal{W}} \mathbf{L}_a^{bt} J$.

However, if we consider more complex properties, the situation is different. Imagine, for example, an environment that is composed not only of the car c, but also other information o. Our epistemic world is thus $o \bullet c$. So, even if we have $c \models_{\mathcal{W}} O$, we cannot use the property $O \to \mathbf{L}_a^{bt} J$ as we don't have $o \bullet c \models_{\mathcal{W}} O$. On the contrary, if we state the

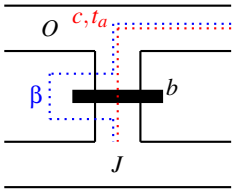

Figure 3. Barrier problem with a shortcut

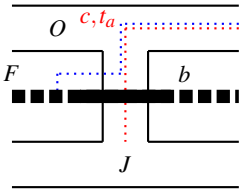

Figure 4. Barrier problem with a fence

property $O \multimap \mathbf{L}_a^{bt} J$ as valid instead, then we have, in particular, $o \models_{\mathcal{W}} O \multimap \mathbf{L}_a^{bt} J$ and, together with $c \models_{\mathcal{W}} O$, this gives $o \bullet c \models_{\mathcal{W}} \mathbf{L}_a^{bt} J$, as desired. So, the use of $\multimap$ instead of $\rightarrow$ is much more useful in more complex systems, as it allows us to set aside, as with Separation Logic's Frame Rule, some of the entities of our system and still apply the property.

Now we introduce agents to the model (see Figure 2). The first model may seem crude, because a single resource is used to model the access of any agent. So, we seek to benefit from the logic that allows us to take agents into account. We change the model by defining a detailed set of agents, $A = \{\alpha, \beta, \gamma\}$ and now take three users, α, β, and γ. Each user should have its own access token, and the resource set is modified accordingly: $Res = \{e, b, t_\alpha, t_\beta, t_\gamma\}$. Now the slightly different formula $O \rightarrow \mathbf{L}_a^{bt_a} J$ is valid for any agent $a \in A$. So, for example, $O \rightarrow \mathbf{L}_\alpha^{bt_\alpha} J$ is valid, which means that α can get inside with his own token, but $O \rightarrow \mathbf{L}_\alpha^{bt_\beta} J$ is not, which means α cannot use β's token.

Now consider that the access is controlled and the agents are supposed to cross the barrier only if they have the appropriate access device. We want to capture the fact that the system can actually be flawed (as mentioned in the problem presentation). It is actually quite easy to do, because being able to circumvent the barrier just means being able to access inside of the complex without any token. We could be a little more specific by imagining that some agents know the shortcut (or dare to use it) and others don't (See Figure 3). In the previous setting, suppose that the agent β is aware of the shortcut and is disposed to use it. Our new set of properties should now be the following:

$$\left\{ O \rightarrow \mathbf{L}_a^{bt_a} J \text{ (for every } a \in A), \; O \rightarrow \mathbf{L}_\beta^{e} J \right\}$$

The unit resource e expresses a direct access (with no resource needed). Note how the use of agents can help us to express different security policies in the same model.

We can reasonably suppose that such a flawed system would be quickly dealt with; for example, by installing a fence that would prevent going around the barrier (See Figure 4). We could, of course, just model that by removing our last addition and get back to the intended policy, but it is more interesting to encode it by a formula. For example, we might then also describe a fault in the fence (or its removal). To do so, we can simply add a propositional formula F that is valid for any resource provided there

is a fence preventing the passage of 'rogue' agents. Our system then becomes

$$\left\{ O \to \mathbf{L}_a^{bt_a} J \text{ (for every } a \in A), \; O \wedge \neg F \to \mathbf{L}_{\beta}^{e} J \right\}$$

Having established a system of formulae that describes our modelling situation quite clearly, we can seek to some properties of the model. The idea is to establish a property of the system that goes beyond its basic definition. For example, we may want to check that every agent inside the facility has passed the barrier and has in its possession its access token. This means that we must prove that, for every agent $a \in A$, $J \to \widetilde{\mathbf{M}}_a^{bt_a} J$.

Indeed, if $c \models_{\mathcal{W}} J \to \widetilde{\mathbf{M}}_a^{bt_a} J$, this means that if $c \models_{\mathcal{W}} J$, then there exists $c' \in R$ such that $c \sim_a c' \bullet b \bullet t_a$ and $c' \bullet b \bullet t_a \models_{\mathcal{W}} J$, which expresses that every resource representing a car that is inside must in fact be equivalent, for a certain agent $a \in A$, to a resource that is inside *and* is composed with both the appropriate token t_a and the barrier token b. This is exactly what we wanted to capture. Notice that this particular property is not verified by the system we stated in the last paragraph. Indeed, as we noticed before, specifying entrance with $r \models_{\mathcal{W}} O \to \mathbf{L}_a^{bt_a} J$ makes J being satisfied by any resource r' such that $r \bullet b \bullet t_a \sim_a r'$. We see that r' does not contain b and t_a. The use of $\mathbf{N}$ instead solves this problem: we then have $r \bullet b \bullet t_a \sim_a r' \bullet b \bullet t_a$ and $r' \bullet b \bullet t_a \models_{\mathcal{W}} J$, as required.

So far, we have consider only simple situations, mainly one car crossing the barrier in various situations. Of course, we may wish to consider more complex models and establish similar properties. For example, we may want to see what happen if several cars are modelled together in the system. We have the sets of properties in the form of implications stated before. To state there is a car in the system, we just assert that the formula O is valid. Then, by looking at the semantics of our formulae, we create a resource c to satisfy that formula. In order to have several cars, we are first tempted to state something like $O \wedge O \wedge O$ (for three cars). However, given our semantics, we have trivially that $O \wedge O \wedge O \equiv O$, which is annoying for our modelling. It is better to state $O * O * O$, using the multiplicative conjunction, instead. Then, to satisfy this formula, we need indeed three resources c_1, c_2, c_3 and we have $c_1 \bullet c_2 \bullet c_3 \models_{\mathcal{W}} O * O * O$. The, using $-\!\!*$ as described above, we can see the system evolve as cars are allowed inside. Thus, the use of $*$ is particularly relevant to model several instances of a same object.

Although we have shown how ERL is sufficiently expressive to describe a security problem and check some of its behavioural properties, the modelling approach described so far quite limited to capturing specific situations in a more-or-less ad hoc manner. One approach to analysing the relationship between policy and system architecture is to reason in terms of *layers*, as developed in [4,5,10], using logics that are similar to, but weaker than, BI. In this set-up, a policy architecture is layered over a system architecture. Another way to think of this that we design first a general model with very few details, and then to design several others that *refine* one another by inheriting the last model's designs while adding some new and more precise details.

5 A Tableaux Calculus for ERL

We define a labelled tableaux calculus for ERL in the spirit of previous work for BI: [11], BBI [16], ESL [7], and ILGL [10]. First, we introduce labels and constraints that

Rules for resource constraints:

$$\frac{}{\varepsilon \simeq \varepsilon}\ \langle \varepsilon \rangle \qquad \frac{x \simeq y}{y \simeq x}\ \langle s_r \rangle \qquad \frac{xy \simeq xy}{x \simeq x}\ \langle d_r \rangle \qquad \frac{x \simeq y \qquad y \simeq z}{x \simeq z}\ \langle t_r \rangle$$

$$\frac{x \simeq y \qquad yk \simeq yk}{xk \simeq yk}\ \langle c_r \rangle \qquad \frac{x =_u y}{x \simeq x}\ \langle k_r \rangle$$

Rules for agent constraints:

$$\frac{x \simeq x}{x =_v x}\ \langle r_a \rangle \qquad \frac{x =_u y}{y =_u x}\ \langle s_a \rangle \qquad \frac{x =_u y \qquad y =_u z}{x =_u z}\ \langle t_a \rangle \qquad \frac{x =_u y \qquad x \simeq k}{k =_u y}\ \langle k_a \rangle$$

Figure 5. Rules for constraint closure (for any $u \in A$)

correspond, respectively, to resources and to the equality and equivalence relations on resources and agents. We consider a finite set of constants Λ_r such that $|\Lambda_r| = |Res| - 1$. On it we build an infinite countable set of (resource) constants γ_r such that $\Lambda_r \subset \gamma_r$, and then $\gamma_r = \Lambda_r \cup \{c_1, c_2, \ldots\}$. Concatenation of lists is denoted by $\oplus$; $[\![]\!]$ denotes the empty list. A *resource label* is a word built on γ_r, where the order of letters is not taken into account; that is, a finite multiset γ_r and by ε the empty word. For example, xy is the composition of the resource labels x and y. We say that x is a *resource sublabel* of y if and only if there exists z such that $xz = y$. The set of resource sublabels of x is denoted $\mathcal{E}(x)$.

We define a function $\lambda : Res \mapsto L_r$ such that: 1. $\lambda(e) = \varepsilon$; 2. for all $r \in Res \backslash \{e\}$, $\lambda(r) \in \Lambda_r$; 3. λ is injective (if $\lambda(r) = \lambda(r')$, then $r = r'$). Note that λ is trivially a bijection between Res and $\Lambda_r \cup \{\varepsilon\}$.

Definition 5 (Constraints). *A* resource constraint *is an expression of the form $x \simeq y$, where x and y are resource labels. An* agent constraint *is an expression of the form $x =_u y$, where x and y are resource labels and u belongs to the set of agents A.*

A *set of constraints* is any set $\mathcal{C}$ that contains resource constraints and agent constraints. Let $\mathcal{C}$ be a set of constraints. The (resource) *domain* of $\mathcal{C}$ is the set of all resource sublabels that appear in $\mathcal{C}$; that is,

$$\mathcal{D}_r(\mathcal{C}) = \bigcup_{x \simeq y \in \mathcal{C}} (\mathcal{E}(x) \cup \mathcal{E}(y)) \cup \bigcup_{x =_u y \in \mathcal{C}} (\mathcal{E}(x) \cup \mathcal{E}(y)).$$

Let $\mathcal{C}$ be a set of constraints. The (resource) *alphabet* $\mathcal{A}_r(\mathcal{C})$ of $\mathcal{C}$ is the set of resource constants that appear in $\mathcal{C}$. In particular, $\mathcal{A}_r(\mathcal{C}) = \gamma_r \cap \mathcal{D}_r(\mathcal{C})$. Now we introduce, in Figure 5, the rules for constraint closure that allow us to capture the properties of the models into the calculus.

Definition 6 (Closure of constraints). *Let $\mathcal{C}$ be a set of constraints. The closure of $\mathcal{C}$, denoted $\overline{\mathcal{C}}$, is the least relation closed under the rules of Figure 5 such that $\mathcal{C} \subseteq \overline{\mathcal{C}}$.*

There are six rules ($\langle \varepsilon \rangle$, $\langle s_r \rangle$, $\langle d_r \rangle$, $\langle t_r \rangle$, $\langle c_r \rangle$, and $\langle k_r \rangle$) that produce resource constraints and four rules ($\langle r_a \rangle$, $\langle s_a \rangle$, $\langle t_a \rangle$, and $\langle k_a \rangle$) that produce agent constraints. We note that v, introduced in the rule $\langle r_a \rangle$, must belong to the set of agents A.

Proposition 3. *The following rules can be derived from the rules of constraint closure:*

$$\frac{xk \simeq y}{x \simeq x}\ \langle p_l\rangle \qquad \frac{x \simeq yk}{y \simeq y}\ \langle p_r\rangle \qquad \frac{xk \eqsim_u y}{x \simeq x}\ \langle q_l\rangle \qquad \frac{x \eqsim_u yk}{y \simeq y}\ \langle q_r\rangle$$

$$\frac{x \eqsim_u y \qquad x \simeq x' \qquad y \simeq y'}{x' \eqsim_u y'}\ \langle w_a\rangle$$

Corollary 1. *Let $\mathcal{C}$ be a set of constraints and $u \in A$ be an agent.*

1. *$x \in \mathcal{D}_r(\overline{\mathcal{C}})$ iff $x \simeq x \in \overline{\mathcal{C}}$ iff $x \eqsim_u x \in \overline{\mathcal{C}}$.*
2. *If $xy \in \mathcal{D}_r(\overline{\mathcal{C}})$, $x' \simeq x \in \overline{\mathcal{C}}$, and $y' \simeq y \in \overline{\mathcal{C}}$, then $xy \simeq x'y' \in \overline{\mathcal{C}}$.*

Proposition 4. *Let $\mathcal{C}$ be a set of constraints. We have $\mathcal{A}_r(\mathcal{C}) = \mathcal{A}_r(\overline{\mathcal{C}})$.*

Lemma 2 (Compactness). *Let $\mathcal{C}$ be a (possibly infinite) set of constraints.*

1. *If $x \simeq y \in \overline{\mathcal{C}}$, then there is a finite set $\mathcal{C}_f$ such that $\mathcal{C}_f \subseteq \mathcal{C}$ and $x \simeq y \in \overline{\mathcal{C}_f}$.*
2. *If $x \eqsim_u y \in \overline{\mathcal{C}}$, then there is a finite set $\mathcal{C}_f$ such that $\mathcal{C}_f \subseteq \mathcal{C}$ and $x \eqsim_u y \in \overline{\mathcal{C}_f}$.*

We define a labelled tableaux calculus for ERL in the spirit of previous work for BI [11], BBI [16], ESL [7], and ILGL [10] by using similar definitions and results.

Definition 7. *A* labelled formula *is a 3-tuple of the form $(\mathbb{S}\phi : x)$ such that $S \in \{\mathbb{T}, \mathbb{F}\}$, $\phi \in \mathcal{L}$ is a formula and $x \in L_r$ is a resource label. A* constrained set of statements *(CSS) is a pair $\langle \mathcal{F}, \mathcal{C}\rangle$, where $\mathcal{F}$ is a set of labelled formulae and $\mathcal{C}$ is a set of constraints, satisfying the property: if $(\mathbb{S}\phi : x) \in \mathcal{F}$, then $x \simeq x \in \overline{\mathcal{C}}$ (call this property P_{css}). A CSS $\langle \mathcal{F}, \mathcal{C}\rangle$ is* finite *if $\mathcal{F}$ and $\mathcal{C}$ are finite. The relation $\preccurlyeq$ is defined by $\langle \mathcal{F}, \mathcal{C}\rangle \preccurlyeq \langle \mathcal{F}', \mathcal{C}'\rangle$ iff $\mathcal{F} \subseteq \mathcal{F}'$ and $\mathcal{C} \subseteq \mathcal{C}'$. We write $\langle \mathcal{F}_f, \mathcal{C}_f\rangle \preccurlyeq_f \langle \mathcal{F}, \mathcal{C}\rangle$ when $\langle \mathcal{F}_f, \mathcal{C}_f\rangle \preccurlyeq \langle \mathcal{F}, \mathcal{C}\rangle$ holds and $\langle \mathcal{F}_f, \mathcal{C}_f\rangle$ is finite, meaning that $\mathcal{F}_f$ and $\mathcal{C}_f$ are both finite.*

Proposition 5. *For any CSS $\langle \mathcal{F}_f, \mathcal{C}\rangle$, where $\mathcal{F}_f$ is finite, there exists $\mathcal{C}_f \subseteq \mathcal{C}$ such that $\mathcal{C}_f$ is finite and $\langle \mathcal{F}_f, \mathcal{C}_f\rangle$ is a CSS.*

Proof. By induction on the number of labelled formulae of $\mathcal{F}_f$ and by Lemma 2.

Figure 6 presents the rules of tableaux calculus for ERL. Note that 'c_i and c_j are new label constants' means $c_i \neq c_j \in \gamma_r \setminus (\mathcal{A}_r(\mathcal{C}) \cup \Lambda_r)$.

Definition 8 (Tableau). *Let $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$ be a finite CSS. A* tableau *for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$ is a list of CSS, called* branches*, inductively built according the following rules:*

1. *The one branch list $[\langle \mathcal{F}_0, \mathcal{C}_0\rangle]$ is a tableau for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$;*
2. *If the list $\mathcal{T}_m \oplus [\langle \mathcal{F}, \mathcal{C}\rangle] \oplus \mathcal{T}_n$ is a tableau for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$ and*

$$\frac{cond\langle \mathcal{F}, \mathcal{C}\rangle}{\langle \mathcal{F}_1, \mathcal{C}_1\rangle \mid \ldots \mid \langle \mathcal{F}_k, \mathcal{C}_k\rangle}$$

is an instance of a rule of Figure 6 for which $cond\langle \mathcal{F}, \mathcal{C}\rangle$ is fulfilled, then the list $\mathcal{T}_m \oplus [\langle \mathcal{F} \cup \mathcal{F}_1, \mathcal{C} \cup \mathcal{C}_1\rangle; \ldots; \langle \mathcal{F} \cup \mathcal{F}_k, \mathcal{C} \cup \mathcal{C}_k\rangle] \oplus \mathcal{T}_n$ is a tableau for $\langle \mathcal{F}_0, \mathcal{C}_0\rangle$.

A tableau *for the formula ϕ is a* tableau *for $\langle \{(\mathbb{F}\phi : c_1)\}, \{c_1 \simeq c_1\}\rangle$.*

$$\frac{(\mathbb{T}\mathbf{I} : x) \in \mathcal{F}}{\langle \emptyset, \{x \simeq \varepsilon\}\rangle}\ \langle \mathbb{T}\mathbf{I}\rangle$$

$$\frac{(\mathbb{T}\neg\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : x)\}, \emptyset\rangle}\ \langle \mathbb{T}\neg\rangle \qquad \frac{(\mathbb{F}\neg\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : x)\}, \emptyset\rangle}\ \langle \mathbb{F}\neg\rangle$$

$$\frac{(\mathbb{T}\phi \wedge \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : x), (\mathbb{T}\psi : x)\}, \emptyset\rangle}\ \langle \mathbb{T}\wedge\rangle \qquad \frac{(\mathbb{F}\phi \wedge \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : x)\}, \emptyset\rangle \mid \langle \{(\mathbb{F}\psi : x)\}, \emptyset\rangle}\ \langle \mathbb{F}\wedge\rangle$$

$$\frac{(\mathbb{T}\phi \vee \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : x)\}, \emptyset\rangle \mid \langle \{(\mathbb{T}\psi : x)\}, \emptyset\rangle}\ \langle \mathbb{T}\vee\rangle \qquad \frac{(\mathbb{F}\phi \vee \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : x), (\mathbb{F}\psi : x)\}, \emptyset\rangle}\ \langle \mathbb{F}\vee\rangle$$

$$\frac{(\mathbb{T}\phi \to \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : x)\}, \emptyset\rangle \mid \langle \{(\mathbb{T}\psi : x)\}, \emptyset\rangle}\ \langle \mathbb{T}\to\rangle \qquad \frac{(\mathbb{F}\phi \to \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : x), (\mathbb{F}\psi : x)\}, \emptyset\rangle}\ \langle \mathbb{F}\to\rangle$$

$$\frac{(\mathbb{T}\phi * \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : c_i), (\mathbb{T}\psi : c_j)\}, \{x \simeq c_i c_j\}\rangle}\ \langle \mathbb{T}*\rangle \qquad \frac{(\mathbb{F}\phi * \psi : x) \in \mathcal{F} \text{ and } x \simeq yz \in \overline{\mathcal{C}}}{\langle \{(\mathbb{F}\phi : y)\}, \emptyset\rangle \mid \langle \{(\mathbb{F}\psi : z)\}, \emptyset\rangle}\ \langle \mathbb{F}*\rangle$$

$$\frac{(\mathbb{T}\phi \mathrel{-\!\!*} \psi : x) \in \mathcal{F} \text{ and } xy \simeq xy \in \overline{\mathcal{C}}}{\langle \{(\mathbb{F}\phi : y)\}, \emptyset\rangle \mid \langle \{(\mathbb{T}\psi : xy)\}, \emptyset\rangle}\ \langle \mathbb{T}\mathrel{-\!\!*}\rangle \qquad \frac{(\mathbb{F}\phi \mathrel{-\!\!*} \psi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : c_i), (\mathbb{F}\psi : xc_i)\}, \{xc_i \simeq xc_i\}\rangle}\ \langle \mathbb{F}\mathrel{-\!\!*}\rangle$$

$$\frac{(\mathbb{T}\mathbf{L}^r_u\phi : x) \in \mathcal{F} \text{ and } x\lambda(r) =_u y \in \overline{\mathcal{C}}}{\langle \{(\mathbb{T}\phi : y)\}, \emptyset\rangle}\ \langle \mathbb{T}\mathbf{L}\rangle \qquad \frac{(\mathbb{F}\mathbf{L}^r_u\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : c_i)\}, \{x\lambda(r) =_u c_i\}\rangle}\ \langle \mathbb{F}\mathbf{L}\rangle$$

$$\frac{(\mathbb{T}\mathbf{M}^r_u\phi : x) \in \mathcal{F} \text{ and } x =_u y\lambda(r) \in \overline{\mathcal{C}}}{\langle \{(\mathbb{T}\phi : y\lambda(r))\}, \emptyset\rangle}\ \langle \mathbb{T}\mathbf{M}\rangle \qquad \frac{(\mathbb{F}\mathbf{M}^r_u\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : c_i\lambda(r))\}, \{x =_u c_i\lambda(r)\}\rangle}\ \langle \mathbb{F}\mathbf{M}\rangle$$

$$\frac{(\mathbb{T}\mathbf{N}^r_u\phi : x) \in \mathcal{F} \text{ and } x\lambda(r) =_u y\lambda(r) \in \overline{\mathcal{C}}}{\langle \{(\mathbb{T}\phi : y\lambda(r))\}, \emptyset\rangle}\ \langle \mathbb{T}\mathbf{N}\rangle \qquad \frac{(\mathbb{F}\mathbf{N}^r_u\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{F}\phi : c_i\lambda(r))\}, \{x\lambda(r) =_u c_i\lambda(r)\}\rangle}\ \langle \mathbb{F}\mathbf{N}\rangle$$

$$\frac{(\mathbb{T}\widetilde{\mathbf{L}}^r_u\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : c_i)\}, \{x\lambda(r) =_u c_i\}\rangle}\ \langle \mathbb{T}\widetilde{\mathbf{L}}\rangle \qquad \frac{(\mathbb{F}\widetilde{\mathbf{L}}^r_u\phi : x) \in \mathcal{F} \text{ and } x\lambda(r) =_u y \in \overline{\mathcal{C}}}{\langle \{(\mathbb{F}\phi : y)\}, \emptyset\rangle}\ \langle \mathbb{F}\widetilde{\mathbf{L}}\rangle$$

$$\frac{(\mathbb{T}\widetilde{\mathbf{M}}^r_u\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : c_i\lambda(r))\}, \{x =_u c_i\lambda(r)\}\rangle}\ \langle \mathbb{T}\widetilde{\mathbf{M}}\rangle \qquad \frac{(\mathbb{F}\widetilde{\mathbf{M}}^r_u\phi : x) \in \mathcal{F} \text{ and } x =_u y\lambda(r) \in \overline{\mathcal{C}}}{\langle \{(\mathbb{F}\phi : y\lambda(r))\}, \emptyset\rangle}\ \langle \mathbb{F}\widetilde{\mathbf{M}}\rangle$$

$$\frac{(\mathbb{T}\widetilde{\mathbf{N}}^r_u\phi : x) \in \mathcal{F}}{\langle \{(\mathbb{T}\phi : c_i\lambda(r))\}, \{x\lambda(r) =_u c_i\lambda(r)\}\rangle}\ \langle \mathbb{T}\widetilde{\mathbf{N}}\rangle \qquad \frac{(\mathbb{F}\widetilde{\mathbf{N}}^r_u\phi : x) \in \mathcal{F} \text{ and } x\lambda(r) =_u y\lambda(r) \in \overline{\mathcal{C}}}{\langle \{(\mathbb{F}\phi : y\lambda(r))\}, \emptyset\rangle}\ \langle \mathbb{F}\widetilde{\mathbf{N}}\rangle$$

Note: c_i and c_j are new label constants, with $c_i, c_j \notin \Lambda_r$.

Figure 6. Rules of the tableaux calculus for ERL.

We remark that a tableau for a formula ϕ verifies the property (P_{css}) of Definition 7 (by the rule $\langle r_a \rangle$) and any application of a rule of Figure 6 provide also a tableau that verifies the property (P_{css}) (in particular by Corollary 2).

In this calculus, we have two particular set of rules. The first set is composed by the rules $\langle \mathbb{T}\mathbf{I} \rangle$, $\langle \mathbb{T}* \rangle$, $\langle \mathbb{F}\!\twoheadrightarrow\! * \rangle$, $\langle \mathbb{F}\mathbf{L} \rangle$, $\langle \mathbb{F}\mathbf{M} \rangle$, $\langle \mathbb{F}\mathbf{N} \rangle$, $\langle \mathbb{T}\widetilde{\mathbf{L}} \rangle$, $\langle \mathbb{T}\widetilde{\mathbf{M}} \rangle$, and $\langle \mathbb{T}\widetilde{\mathbf{N}} \rangle$, that introduce new label constants (c_i and c_j) and new constraints, except for $\langle \mathbb{T}\mathbf{I} \rangle$ that only introduces a new constraint. The second set is composed of the rules $\langle \mathbb{F}* \rangle$, $\langle \mathbb{T}\!\twoheadrightarrow\! * \rangle$, $\langle \mathbb{T}\mathbf{L} \rangle$, $\langle \mathbb{T}\mathbf{M} \rangle$, $\langle \mathbb{T}\mathbf{N} \rangle$, $\langle \mathbb{F}\widetilde{\mathbf{L}} \rangle$, $\langle \mathbb{F}\widetilde{\mathbf{M}} \rangle$, and$\langle \mathbb{F}\widetilde{\mathbf{N}} \rangle$, that have a condition on the closure of constraints. To apply one of these rules we choose a label which satisfies the condition and then apply the corresponding rule. Otherwise, we cannot apply the rule.

Definition 9 (Closure condition). *A CSS $\langle \mathcal{F}, \mathcal{C} \rangle$ is* closed *if one of the following conditions holds, where $\phi \in \mathcal{L}$: 1. $(\mathbb{T}\phi : x) \in \mathcal{F}$, $(\mathbb{F}\phi : y) \in \mathcal{F}$ and $x \simeq y \in \overline{\mathcal{C}}$; 2. $(\mathbb{F}\mathbf{I} : x) \in \mathcal{F}$ and $x \simeq \varepsilon \in \overline{\mathcal{C}}$; 3. $(\mathbb{F}\top : x) \in \mathcal{F}$; and 4. $(\mathbb{T}\bot : x) \in \mathcal{F}$. A CSS is* open *if it is not closed. A tableau for ϕ is* closed *if all its branches are closed and a* tableaux proof *for ϕ is a closed tableau for ϕ.*

To illustrate the construction of tableaux, we consider $\mathbf{M}^s_a\phi \to \mathbf{M}^r_a(\mathbf{M}^s_a\phi)$. To build the corresponding tableau, we start with the CCS $\langle \{(\mathbb{F}\mathbf{M}^s_a\phi \to \mathbf{M}^r_a(\mathbf{M}^s_a\phi) : c_1)\}, \{c_1 \simeq c_1\} \rangle$ and with the following representation of the formula set $\mathcal{F}$ and the constraints set $\mathcal{C}$:

$$\begin{array}{cc} [\mathcal{F}] & [\mathcal{C}] \\ \surd_1(\mathbb{F}\mathbf{M}^s_a\phi \to \mathbf{M}^r_a(\mathbf{M}^s_a\phi) : c_1) & c_1 \simeq c_1 \end{array}$$

We then apply the rules of our tableaux method, respecting the priority order, and we obtain the tableau of Figure 7. We omit the λ and write r for $\lambda(r)$, for any resource.

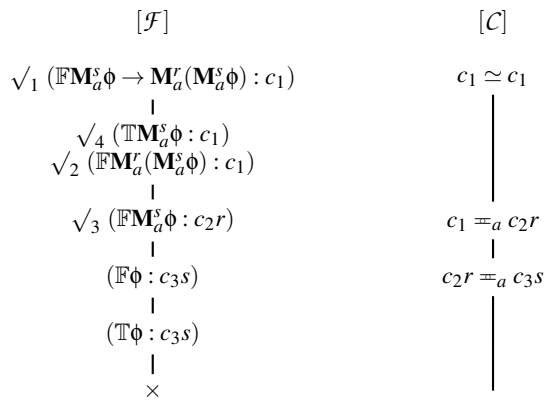

Figure 7. Tableau for $\mathbf{M}^s_a\phi \to \mathbf{M}^r_a(\mathbf{M}^s_a\phi)$

Note that we mark with $\surd$ the steps of the tableau construction. The main steps are the following: first apply the rule $\langle \mathbb{F} \to \rangle$ and then obtain two formulae both with $\mathbf{M}$ as

operator. According to the priority rules, first apply the $\langle \mathbb{F}\mathbf{M} \rangle$ rule, which generates a new formula, a new resource label c_2, and the constraint $c_1 \eqcirc_a c_2 r$. Then apply the $\langle \mathbb{F}\mathbf{M} \rangle$ rule again, which generates a new formula, a new resource label c_3, and the constraint $c_2 r \eqcirc_a c_3 s$. We must now apply the $\langle \mathbb{T}\mathbf{M} \rangle$ rule and then we need a resource label z such that $c_1 \eqcirc_a zs \in \overline{\mathcal{C}}$. Now, having closure by rule $\langle t_a \rangle$ with agent a, we generate the constraint $c_1 \eqcirc_a c_3 s$, and thus apply the rule with $z = c_1$ and generate $(\mathbb{T}\phi : c_3 s)$. As we also have $(\mathbb{F}\phi : c_3 s)$, we have a closed branch and thus a closed tableau.

Theorem 1 (Soundness). *Let ϕ be a formula of ERL. If there exists a tableaux proof for ϕ, then ϕ is valid.*

Proof. The proof is similar to the soundness proof of BI tableaux [11] and its recent extensions [6,7,10]. The main point is the notion of *realizability* of a CSS $\langle \mathcal{F}, \mathcal{C} \rangle$, meaning that there exists a model $\mathcal{M}$ and an embedding $(|.|)$ from the resource labels to the resource set of $\mathcal{M}$ such that if $(\mathbb{T}\phi : x) \in \mathcal{F}$, then $|x| \vDash_{\mathcal{M}} \phi$,and if $(\mathbb{F}\phi : x) \in \mathcal{F}$, then $|x| \nvDash_{\mathcal{M}} \phi$. More details are given in [12].

We propose a countermodel extraction method, adapted from [16], that transforms the sets of resource and agent constraints of a branch $\langle \mathcal{F}, \mathcal{C} \rangle$ into a model $\mathcal{M}$ such that if $(\mathbb{T}\phi : x) \in \mathcal{F}$, then $\rho_x \vDash_{\mathcal{M}} \phi$, and if $(\mathbb{F}\phi : x) \in \mathcal{F}$, then $\rho_x \nvDash_{\mathcal{M}} \phi$, where ρ_x is the representative of the equivalence class of x.

More details are given in [12] and examples of countermodels with a similar method are given in [6–8,10,11].

Theorem 2 (Completeness). *Let ϕ be an ERL formula. If ϕ is valid, then there exists a tableaux proof for ϕ.*

Proof. The proof consists in building, using a fair strategy, a Hintikka CSS from a formula for which there is no tableaux proof that is a sequence of labelled formulae in which all labelled formulae occur infinitely many times, and an oracle that is a set of non-closed CSS with some specific properties. Then, assuming there is no tableaux proof for ϕ, we build a Hintikka CSS, and deduce from it that ϕ is not valid. More details are given in [12].

6 Conclusions

We have presented a substructural epistemic logic, based on Boolean BI, in which the epistemic modalities, which extend the usual epistemic modalities, are parametrized on the agent's local resource. The logic represents a first step in developing an epistemic resource semantics. This step is illustrated through an example that explores the gap between policy and implementation in access control. We have provided a system of labelled tableaux for the logic, and established soundness and completeness.

Much further work is suggested. First, the theory, pragmatics, and interpretation of the epistemic modalities with resource semantics, including aspects of local reasoning for resource-carrying agents [15,21], concurrency [18]. Second, logical theory, including proof systems, model-theoretic properties, and complexity. Connections with other approaches to modelling the relationship between policy and implementation in system management, such as those discussed in [23] and approaches involving logics for layered graphs [1,4], should be explored.

References

1. G. Anderson and D. Pym. A calculus and logic of bunched resources and processes. *Theoretical Computer Science*, 614:63–96, 2016.
2. A. Baltag, B. Coecke and M. Sadrzadeh. Epistemic Actions as Resources *Journal of Logic and Computation*, 17(3):555-585, 2006.
3. M. Collinson, B. Monahan, and D. Pym. *A Discipline of Mathematical Systems Modelling*. College Publications, 2012.
4. M. Collinson, K. McDonald, and D. Pym. Layered graph logic as an assertion language for access control policy models. *Journal of Logic and Computation*, 2015. doi:10.1093/logcom/exv020.
5. M. Collinson, K. McDonald, and D. Pym. A substructural logic for layered graphs. *Journal of Logic and Computation*, 24(4):953–988, 2014.
6. J-R. Courtault and D. Galmiche. A Modal Separation Logic for Resource Dynamics. *Journal of Logic and Computation*, 46 pages, 2015. doi:10.1093/logcom/exv031.
7. J-R. Courtault, H. van Ditmarsch, and D. Galmiche. An epistemic separation logic. In *22nd International Workshop on Logic, Language, Information, and Computation, WoLLIC 2015, Bloomington, USA, July 2015*. LNCS 9160, 156–173.
8. J.-R. Courtault, D. Galmiche, and D. Pym. A logic of separating modalities. *Theoretical Computer Science* 637, 30–58, 2016. doi: 10.1016/j.tcs.2016.04.040.
9. H. van Ditmarsch, J.Y. Halpern, W. van der Hoek, and B. Kooi (editors). *Handbook of Epistemic Logic*. College Publications, 2015.
10. S. Docherty and D. Pym. Intuitionistic Layered Graph Logic. *Proc. IJCAR 2016*, Coimbra, Portugal. LNCS 9706, 469–486, 2016. doi:10.1007/978-3-319-40229-1_32.
11. D. Galmiche, D. Méry, and D. Pym. The semantics of BI and Resource Tableaux. *Math. Struct. Comp. Sci.* 15(6):1033–1088, 2005.
12. D. Galmiche, P. Kimmel, and D. Pym. A Substructural Epistemic Resource Logic (Extended Version) UCL Research Note RN/16/08, 2016. `http://www.cs.ucl.ac.uk/fileadmin/UCL-CS/research/Research_Notes/RN_16_08.pdf`
13. J. Halpern and R. Pucella. Modeling adversaries in a logic for security protocol analysis. LNCS 2629,115–132, 2003.
14. P. O'Hearn and D. Pym. The logic of Bunched Implications. *Bulletin of Symbolic Logic* 5(2):215-244, 1999.
15. S. Ishtiaq and P. O'Hearn. BI as an assertion language for mutable data structures. In *28th ACM Symposium on Principles of Programming Languages (POPL)*, London, 2001, 14–26.
16. D. Larchey-Wendling. The formal strong completeness of partial monoidal Boolean BI. *Journal of Logic and Computation* 26(2), 605–640, 2014. doi: 10.1093/logcom/exu031
17. P. Naumov and J. Tao. Budget-constrained Knowledge in Multiagent Systems. In *Proc. AAMAS 2015*, 219–226, 2015.
18. P.W. O'Hearn. Resources, Concurrency and Local Reasoning. *Theoretical Computer Science* 375(1-3), 271–307, 2007.
19. R. Pucella. Knowledge and Security. Chapter 12 of [9], 591–655.
20. D. Pym, P. O'Hearn, and H. Yang. Possible worlds and resources: the semantics of BI. *Theoretical Computer Science* 315(1): 257–305. Erratum: p. 22, l. 22 (preprint), p. 285, l. -12 (TCS): ', for some P' , $Q \equiv P; P'$' should be '$P \vdash Q$'.
21. J. Reynolds. Separation logic: A logic for shared mutable data structures. In *IEEE Symposium on Logic in Computer Science, LICS 2002*, 55–74, Copenhagen, Denmark, July 2002.
22. B. Schneier. The weakest link (`https://www.schneier.com/blog/archives/2005/02/the_weakest_lin.html`). Schneier on Security (`https://www.schneier.com`), 2005.
23. B. Toninho and L. Caires. A spatial-epistemic logic for reasoning about security protocols. In *8th Int. Workshop on Security Issues in Concurrency, SecCo 2010*, 2010.